U.O.C. Ingegneria Informatica.
Direttore ing. Salvatore Garozzo

REGOLAMENTO AZIENDALE SULL'ACCESSO AD INTERNET E SULL'USO DELLA POSTA ELETTRONICA - POLICY AZIENDALE

PREMESSA

Il Garante per la protezione dei dati personali, con Provvedimento del 1.03.2007 pubblicato sulla G. U. R.I. del 10.03.2007, n. 58, ad oggetto *"Trattamento di dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori"* raccomanda l'adozione da parte dei datori di lavoro pubblici e privati, di un disciplinare interno, in cui siano indicate le regole per l'uso di Internet, della posta elettronica e della tenuta di file della rete interna nel rispetto del Decreto Legislativo 30.06.2003, n. 196 (Codice in materia di protezione dei dati personali).

Sono altresì regolate le modalità con le quali l'Asp di Catania può accertare e inibire le condotte illecite degli utilizzatori di Internet, della posta elettronica e dell'accesso alle risorse di archiviazione di massa (server – hard disk).

La realtà aziendale è andata caratterizzandosi in questi ultimi anni per l'elevato uso delle tecnologie informatiche che se da un lato hanno consentito l'introduzione di innovative tecniche di gestione, dall'altro hanno anche dato origine a numerose problematiche relative all'utilizzo degli strumenti informatici forniti dall'azienda ai propri dipendenti per lo svolgimento delle mansioni e compiti affidati.

In questo senso, viene fortemente sentita la necessità di porre in essere adeguati sistemi di controllo sull'utilizzo di tali strumenti da parte dei dipendenti/collaboratori e di sanzionare conseguentemente quegli usi scorretti che, oltre ad esporre l'Azienda stessa a rischi tanto patrimoniali quanto penali, possono di per sé considerarsi contrari ai doveri di diligenza e fedeltà previsti dagli artt. 2104 e 2105 del Codice civile.

I controlli sull'uso degli strumenti informatici tuttavia, devono garantire tanto il diritto del datore di lavoro di proteggere la propria organizzazione, essendo i computer aziendali strumenti di lavoro la cui utilizzazione personale è preclusa, quanto il diritto del lavoratore a non vedere invasa la propria sfera personale, e quindi il diritto alla riservatezza ed alla dignità come sanciti dallo Statuto dei lavoratori e dal Codice sulla privacy.

Il regolamento aziendale, quale quello proposto, ed in genere le "policy" aziendali che dettano le regole sull'uso degli strumenti informatici e telematici, non sono comunque sostitutive della procedura prevista dal 2° comma dell'art. 4 dello Statuto dei lavoratori in materia di controlli leciti, nei casi in cui questa procedura sia necessaria.

Si evidenzia, inoltre, che l'accesso da parte del datore di lavoro ai messaggi di posta elettronica presenti nella casella di posta assegnata ai singoli dipendenti potrebbe, potenzialmente, determinare violazione dell'art. 616 del codice penale, che punisce la violazione, sottrazione e soppressione di corrispondenza anche telematica altrui.

Tuttavia, proprio l'adozione di un regolamento aziendale che evidenzi la natura non personale della casella di posta assegnata e ne definisca le modalità d'uso ed i possibili controlli, rappresenta un utile strumento per evitare la configurabilità di tale reato.

Alla luce delle considerazioni sopra espresse e tenuto opportunamente conto delle Linee guida emanate dall'Autorità Garante per la protezione dei dati personali, con propria deliberazione n.13 del 1 marzo 2007, sulla disciplina della navigazione in internet e sulla gestione della posta elettronica nei luoghi di lavoro, l'Azienda Sanitaria Provinciale di Catania ha predisposto il regolamento per disciplinare le condizioni per il corretto utilizzo degli strumenti informatici da parte dei suoi dipendenti e/o collaboratori.

Il regolamento di seguito proposto, essendo rilevante ai fini delle eventuali azioni disciplinari attivabili dal datore di lavoro nei confronti del dipendente, è stato redatto tenendo opportunamente conto delle normative vigenti in merito.

Vengono inoltre considerati gli specifici obblighi previsti dal Codice della privacy (D.Lgs. n. 196/2003 e successive modifiche ed integrazioni) e dall'art. 29, 1° comma del D.Lgs. n. 242/1996 (in tema di controlli operati mediante il sistema informatico aziendale), nonché gli obblighi previsti dal disciplinare tecnico sulle misure minime di sicurezza allegato allo stesso Codice.

U.O.C. Ingegneria Informatica.
Direttore ing. Salvatore Garozzo

Con riferimento alle normativa in tema di protezione dei dati personali, si ricorda come il Codice della privacy stabilisce che l'attività di controllo debba essere rispettosa dei principi fondamentali di "proporzionalità" (art. 3), debba avvenire nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato (art.2) e soprattutto, che di tale attività, debba essere fornita adeguata e preventiva informativa (art. 13).

Il regolamento oltre a dettare una disciplina per l'utilizzo degli strumenti informatici aziendali, vuole costituire un utile strumento per sensibilizzare il personale su altri aspetti altrettanto importanti nella gestione dei sistemi informatici aziendali, quali il rispetto della normativa sulla tutela legale del software (e quindi il controllo sulla regolarità del software presente nello stesso sistema informatico), e quella sulla tutela del know-how aziendale, quando queste importanti informazioni di proprietà dell'Azienda sono custodite nel sistema informatico.

Il regolamento sarà pubblicizzato adeguatamente e verrà sottoposto ad aggiornamento periodico.

Sono tenuti all'osservanza delle presenti disposizioni i Direttori/Responsabili di Struttura, tutti i Dipendenti dell'Azienda, nonché gli "esterni" all'ASP Catania anche nei casi relativi a collaborazione di persone fisiche o giuridiche (convenzioni, consulenze, tirocini, appalti etc.).

INTRODUZIONE

La progressiva diffusione delle nuove tecnologie informatiche e, in particolare, il libero accesso alla rete Internet dai Personal Computer, espone l'azienda e gli utenti (dipendenti e collaboratori della stessa) a rischi di natura patrimoniale, oltre alle responsabilità penali conseguenti alla violazione di specifiche disposizioni di legge (legge sul diritto d'autore e legge sulla privacy, fra tutte), creando evidenti problemi alla sicurezza ed all'immagine dell'Azienda stessa.

Premesso quindi che l'utilizzo delle risorse informatiche e telematiche deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito dei rapporti di lavoro, l'Azienda adotta questo Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza informatica e al trattamento dei dati.

U.O.C. Ingegneria Informatica.
Direttore ing. Salvatore Garozzo

L'uso di Internet nelle sue numerose funzionalità è consentito esclusivamente per gli scopi attinenti al proprio lavoro.

Data la vasta gamma di attività aziendali, non è stato definito a priori un elenco di siti autorizzati; si è tuttavia optato per l'utilizzo di appositi strumenti di filtraggio, mediante i quali è stata bloccata la navigazione su categorie di siti i cui contenuti sono stati classificati come certamente estranei agli interessi ed alle attività aziendali.

Il divieto di accesso ad un sito appartenente alle categorie inibite viene visualizzato esplicitamente a video.

Viene altresì limitata la possibilità di scaricare (download) da Internet file musicali, video o software che non siano necessari alla propria attività aziendale.

Viene tassativamente vietato l'utilizzo delle risorse dei server aziendali per la memorizzazione di materiale privato, personale o non attinente all'attività lavorativa.

Relativamente all'utilizzo dei singoli Personal Computer si precisa che l'assegnazione della risorsa non ne comporta la privatezza, in quanto trattasi di strumento di esclusiva proprietà aziendale, e quindi i files memorizzati non sono né tutelati né garantiti dall'Asp di Catania per qualsiasi causa.

L'autorizzazione all'accesso alla rete internet è richiesta dall'utente al proprio responsabile che, a seguito di una necessaria valutazione, potrà dare parere favorevole e richiedere alla UOC Ingegneria Informatica le relative credenziali da assegnare all'utente.

L'accesso è consentito a seguito di rilascio di credenziali di dominio.

Le prescrizioni di seguito previste si aggiungono ed integrano le specifiche istruzioni già fornite con:

- Ordine di Servizio n 140 del 2 settembre 2008
- Deliberazione n. 134 del 29 gennaio 2010 riguardante "Regolamento aziendale sulla sicurezza informatica".

DEFINIZIONI

Ai fini delle disposizioni dettate per l'utilizzo delle risorse informatiche e telematiche, per "**utente**" deve intendersi ogni dipendente e collaboratore (collaboratore a progetto, dipendenti ditte

esterne, in stage, volontario, tirocinante etc.) in possesso di specifiche credenziali di autenticazione rilasciate dalla Unità Operativa Complessa Ingegneria Informatica.

Tale figura potrà anche venir indicata quale "incaricato del trattamento". I successivi acronimi sono così definiti:

1. **UOC IngInf**: Unità Operativa Complessa Ingegneria Informatica,
2. **Azienda**: ASP Catania.

CAMPO DI APPLICAZIONE DEL REGOLAMENTO

Il regolamento si applica a tutti i dipendenti, senza distinzione di ruolo e/o livello, nonché a tutti i collaboratori dell'azienda a prescindere dal rapporto contrattuale con la stessa intrattenuto (collaboratore a progetto, in stage, consulenti, tirocinanti ecc.).

Copia del regolamento, oltre ad essere spedito a tutte le e-mail aziendali @aspct.it, verrà pubblicato sul sito intranet aziendale *intranet.aspct.it* *.

** La consegna di una copia è una scelta facoltativa dell'Azienda: in caso di consegna a mano, la premessa del presente regolamento può anche essere riportata in un'eventuale lettera di accompagnamento. Si ricorda infatti che ai sensi dell'art. 7 Legge n. 300/1970 l'unico obbligo a carico del datore di lavoro,* ***ai fini dell'esercizio del potere disciplinare****, è quello di dare adeguata pubblicità delle norme mediante l'affissione in luogo accessibile a tutti.*

UTILIZZO DEL PERSONAL COMPUTER

Il Personal Computer affidato all'utente è uno strumento di lavoro. Ogni utilizzo non inerente all'attività lavorativa è vietato perché può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

Il personal computer deve essere utilizzato con cura evitando ogni possibile forma di danneggiamento e permette l'accesso alla rete aziendale solo attraverso specifiche credenziali di autenticazione come meglio descritto nei successivi articoli del presente Regolamento.

U.O.C. Ingegneria Informatica.
Direttore ing. Salvatore Garozzo

L'Azienda rende noto che il personale incaricato che opera presso la **UOC IngInf** della stessa Azienda è stato autorizzato a compiere interventi nel sistema informatico aziendale diretti a garantire la sicurezza e la salvaguardia del sistema stesso, nonché per ulteriori motivi tecnici e/o manutentivi (ad es. aggiornamento/sostituzione/implementazione di programmi, manutenzione hardware etc.).

Il personale incaricato della **UOC IngInf** ha la facoltà di collegarsi e visualizzare in remoto il desktop delle singole postazioni PC al fine di garantire l'assistenza tecnica e la normale attività operativa nonché la massima sicurezza contro virus, spyware, malware, etc. L'intervento viene effettuato esclusivamente su chiamata dell'utente (l'attività di assistenza e manutenzione avviene previa autorizzazione telefonica da parte dell'utente interessato) o, in caso di oggettiva necessità**,** a seguito della rilevazione tecnica di problemi nel sistema informatico e telematico. In quest'ultimo caso, e sempre che non si pregiudichi la necessaria tempestività ed efficacia dell'intervento, verrà data comunicazione della necessità dell'intervento stesso. La configurazione del software prevede un indicatore visivo sul monitor dell'utente che segnala quando il tecnico è connesso al personal computer.

Come già specificato nel regolamento di cui alla Deliberazione n. 134 del 29 gennaio 2010, non è consentito l'uso di programmi diversi da quelli autorizzati dall'Azienda, né viene consentito agli utenti di installare autonomamente programmi provenienti dall'esterno, sussistendo infatti il grave pericolo di introdurre Virus informatici e/o di alterare la funzionalità delle applicazioni software esistenti. L'inosservanza della presente disposizione può esporre a gravi responsabilità civili.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il personale della **UOC IngInf** nel caso in cui siano rilevati virus.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio o in caso di suo inutilizzo. In ogni caso, lasciare un elaboratore incustodito e connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso ***.**

** Una modalità automatica che evita di lasciare incustodito il pc, anche in caso di mancato spegnimento da parte dell'utente è quello di adottare il savescreen a tempo con obbligo di reintrodurr*

e la password per l'accesso.

GESTIONE ED ASSEGNAZIONE DELLE CREDENZIALI DI AUTENTICAZIONE

Le credenziali di autenticazione per l'accesso al PC vengono assegnate al dipendente dal personale della **UOC IngInf**, previa formale richiesta del Direttore del Servizio nell'ambito del quale il nuovo utente verrà inserito ed andrà ad operare.

Nel caso di collaboratori a progetto e coordinati e continuativi la preventiva richiesta, se necessaria, verrà inoltrata direttamente dalla Direzione Aziendale (ovvero dal Responsabile dell'ufficio o area con il quale il collaboratore si coordina nell'espletamento del proprio incarico).

Le credenziali di autenticazione consistono in un codice per l'identificazione dell'utente (user id), assegnato dalla **UOC IngInf** associato ad una parola chiave (password) riservata che dovrà venir custodita dall'incaricato con la massima diligenza e non divulgata..

La parola chiave, formata da lettere (maiuscole o minuscole) e/o numeri, anche in combinazione fra loro, deve essere composta da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato.

È necessario procedere alla modifica della parola chiave a cura dell'utente, incaricato del trattamento, al primo utilizzo e, successivamente, almeno ogni sei mesi (Ogni tre mesi nel caso invece di trattamento di dati sensibili attraverso l'ausilio di strumenti elettronici).

Qualora la parola chiave dovesse venir sostituita, per decorso del termine sopra previsto e/o in quanto abbia perduto la propria riservatezza, si procederà in tal senso d'intesa con il personale della **UOC IngInf.**

Il personale della **UOC IngInf** può in qualunque momento procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Risulta opportuno che, con regolare periodicità (almeno ogni tre mesi), ciascun utente provveda alla pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati, essendo infatti necessario evitare un'archiviazione ridondante.

UTILIZZO E CONSERVAZIONE DEI SUPPORTI RIMOVIBILI

Tutti i supporti rimovibili (dischetti, CD e DVD riscrivibili, supporti USB, ecc.), contenenti dati sensibili nonché informazioni costituenti know-how aziendale, devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere trafugato o alterato e/o distrutto o, successivamente alla cancellazione, recuperato.

Al fine di assicurare la distruzione e/o inutilizzabilità di supporti magnetici rimovibili contenenti dati sensibili, ciascun utente potrà contattare il personale della **UOC IngInf** e seguire le istruzioni da questo impartite.

In ogni caso, i supporti contenenti dati sensibili devono essere dagli utenti adeguatamente custoditi in armadi chiusi.

L'utente è responsabile della custodia dei supporti e dei dati aziendali in essi contenuti.

UTILIZZO DI PC PORTATILI

L'utente è responsabile del PC portatile assegnatogli e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo nel luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste dal presente regolamento, con particolare attenzione alla rimozione di eventuali file elaborati prima della riconsegna.

I PC portatili utilizzati all'esterno, in caso di allontanamento, devono essere custoditi con diligenza, adottando tutti i provvedimenti che le circostanze rendono necessari per evitare danni o sottrazioni.

GESTIONE DEL SERVIZIO

Della gestione delle risorse informatiche così come dell'abilitazione per la connessione ad internet ed del servizio di posta elettronica è responsabile la **UOC IngInf**.

La **UOC IngInf** è tenuto a:

- Adottare le misure più idonee a garantire continuità, disponibilità e sicurezza del servizio
- Gestire i dati degli utenti nel rispetto della vigente normativa sulla tutela dei dati personali

- Informare tempestivamente gli utenti con anticipo di eventuali fermi o interruzioni di servizio che si rendessero necessari per manutenzione o per cause di forza maggiore
- Monitorare i livelli di servizio al fine di garantire la massima efficienza
- Garantire la funzionalità tecnica

In particolare cura:

1. l'attribuzione e la revoca di account e di password e la gestione dei livelli di accesso.
2. l'individuazione delle risorse informatiche e software relativamente agli acquisti ed il collaudo di tutte le attrezzature informatiche, telematiche e software.
3. l'assegnazione – come richiesto ed autorizzato dal responsabile della Struttura presso la quale il dipendente è in servizio - del numero degli accessi ad internet sulla base delle effettive necessità e compatibilmente con la banda minima da garantire per le normali attività dell'azienda.
3. la configurazione e l'amministrazione delle risorse informatiche e reti. Per risorse informatiche si intendono:
    - macchine del Settore Informatico (installate presso il settore e/o presso la sala Server); workstation, personal computer, notebook , stampanti utilizzati da dipendenti, amministratori, personale con incarichi professionali, stagisti, tirocinanti ed eventuali ospiti;
    - tutte le macchine facenti comunque parte della rete;
    - apparati di rete;
    - tutto il software e i dati acquistati o prodotti per l'amministrazione dei sistemi, per l'utilizzo da parte degli utenti o di terzi autorizzati.
5. la revoca dell'accesso temporaneo alla risorsa Informatica e di rete, sentito il Dirigente preposto, qualora questo sia utilizzato impropriamente o in violazione delle leggi vigenti; potrà altresì interrompere temporaneamente la prestazione del servizio in presenza di motivati problemi di sicurezza, riservatezza o guasto tecnico, dandone tempestiva comunicazione all'utente.
6. l'Attivazione/disattivazione della casella di Posta Elettronica personale per il dipendente, autorizzato dal dirigente responsabile.

7. l'Attivazione/disattivazione della casella di Posta Elettronica per i collaboratori, previa richiesta del dirigente della struttura di afferenza;
8. l'Attivazione/disattivazione della casella di Posta Elettronica di servizio/struttura a seguito di modifica organizzativa dell'Azienda per variazione organizzativa come da atto aziendale

Il Personale della **UOC IngInf** può accedere in qualsiasi momento, anche senza preavviso, ai locali e alle risorse informatiche dell' Azienda sia in caso di emergenza, sia per effettuare gli interventi di assistenza, verifica e supporto.

La **UOC IngInf** non effettua alcuna misura, controllo, censura, modifica, cancellazione di messaggi sui server di posta elettronica tranne quando ciò è legato a:

- esigenze tecniche o di sicurezza del tutto particolari;
- indispensabilità del dato rispetto all'esercizio o alla difesa di un diritto in sede giudiziaria;
- obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell'autorità giudiziaria o della Polizia Postale.

Vige comunque l'assoluto divieto di effettuare controlli con le seguenti modalità:

- la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
- la riproduzione e l'eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
- la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;

ACCESSO A INTERNET E USO DELLA RETE AZIENDALE

La navigazione in internet ed il sistema di posta elettronica sono mezzi di comunicazione, informazione e trasmissione.

U.O.C. Ingegneria Informatica.
Direttore ing. Salvatore Garozzo

L'uso di Internet nelle sue numerose funzionalità è consentito esclusivamente per gli scopi attinenti al proprio lavoro e le attività svolte mediante la navigazione in internet o il sistema di posta elettronica sono destinati al conseguimento dei fini istituzionali dell'Azienda.

I dati che vengono inviati mediante il sistema aziendale di posta elettronica sono di proprietà dell'Azienda.

La banda Internet ed il sistema di posta elettronica sono operanti con continuità, 24 ore al giorno per 365 giorni all'anno.

Per l'accesso alla rete ciascun utente **deve** essere in possesso delle specifiche credenziali di autenticazione (ID utente) e una parola chiave segreta (password).

È assolutamente proibito entrare nella rete e nei programmi con un codice d'identificazione utente diverso da quello assegnato. Le parola chiave d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite.

Superato il sistema di autenticazione l'utente è collegato alla rete aziendale e ad internet senza ulteriori formalità.

Tutti gli utenti connessi ad internet sono tracciati tramite un sistema di sicurezza aziendale che genera un file di "log", nel quale sono registrate tutte le attività svolte dall'utente connesso.

Sempre nel rispetto della protezione dei dati personali, tale file non è visionabile da amministratori di sistema ne da alcun operatore della UOC IngInf, ma è disponibile alla consultazione solo dell'autorità giudiziaria o Polizia Postale in caso di segnalato abuso.

Tutti gli utenti cui è assegnata una postazione di lavoro possono utilizzare internet, su autorizzazione del loro Responsabile e/o Direttore, compatibilmente con le bande a disposizione e previa identificazione con le modalità ID UTENTE / PASSWORD.

Data la vasta gamma di attività aziendali, non è definito a priori un elenco di siti aziendali autorizzati; al fine di prevenire il rischio di utilizzi impropri della rete, l'Azienda utilizza un sistema di filtri che impediscono l'accesso diretto a siti che non hanno natura istituzionale (BLACK LIST: categorie di siti i cui contenuti sono stati classificati come certamente estranei agli interessi ed alle attività aziendali).

Il divieto di accesso ad un sito appartenente alle categorie inibite viene visualizzato esplicitamente a video.

L'utilizzo di internet è autorizzato per ogni singolo utente dalla **UOC IngInf**, previa richiesta adeguatamente motivata controfirmata dal Responsabile e/o Direttore di Struttura.

Il collegamento alla rete da una postazione di lavoro avviene con l'utilizzo della coppia ID utente - password personale.

L'utente si impegna a:

- non cedere, una volta superata la fase di autenticazione, l'uso della propria stazione a personale non autorizzato, in particolar modo per quanto riguarda l'accesso a internet e ai servizi di posta elettronica;
- non lasciare incustodita ed accessibile la propria postazione una volta connesso al sistema con le proprie credenziali di autenticazione;
- conservare la password con la massima riservatezza e diligenza;
- non utilizzare credenziali (ID utente e password) di altri utenti, nemmeno se fornite volontariamente o di cui si ha casualmente conoscenza;

Di qualsiasi azione o attività svolta utilizzando il codice identificativo e/o la password assegnata è responsabile l'utente assegnatario del codice.

Il PC assegnato al singolo utente e abilitato alla navigazione in Internet costituisce uno strumento aziendale utilizzabile esclusivamente per lo svolgimento della propria attività lavorativa.

USO DELLA POSTA ELETTRONICA

La casella di posta elettronica assegnata all'utente è uno strumento di lavoro. Le persone assegnatarie delle caselle di posta elettronica sono responsabili del corretto utilizzo delle stesse.

La casella di posta deve essere mantenuta in ordine, cancellando documenti inutili e soprattutto allegati ingombranti come dimensione

Ogni comunicazione inviata o ricevuta che abbia contenuti rilevanti o contenga impegni contrattuali o precontrattuali per l'Azienda ovvero contenga documenti da considerarsi riservati in quanto contraddistinti dalla dicitura "strettamente riservati" o da analoga dicitura, deve essere visionata anche dal Direttore della Struttura.

È possibile utilizzare la ricevuta di ritorno per avere la conferma dell'avvenuta lettura del messaggio da parte del destinatario.

È obbligatorio porre la massima attenzione nell'aprire i file allegati alla posta elettronica prima del loro utilizzo (non eseguire download di file eseguibili o documenti da siti Web o Ftp non conosciuti).

L'accesso alla posta elettronica è personale e vi si passa tramite nome utente e password di identificazione.

L'accesso non può essere condiviso o ceduto.

PROTEZIONE ANTIVIRUS

Il sistema informatico dell'azienda è protetto da software antivirus aggiornato quotidianamente. Ogni utente deve comunque tenere comportamenti tali da ridurre il rischio di attacco al sistema informatico aziendale mediante virus o mediante ogni altro software aggressivo.

Nel caso in cui il software antivirus rilevi la presenza di un virus, l'utente dovrà immediatamente sospendere ogni elaborazione in corso senza spegnere il computer nonché segnalare prontamente l'accaduto al personale della **UOC IngInf.**

Ogni dispositivo usb o supporto di qualsivoglia natura, di provenienza esterna all'Azienda, dovrà essere verificato mediante il programma antivirus prima del suo utilizzo e, nel caso venga rilevato un virus, dovrà essere prontamente consegnato al personale della **UOC IngInf**.

Nel caso in cui nella postazione di lavoro non sia installato il software antivirus, sarà compito dell'utente segnalarlo alla **UOC IngInf.**

COMPITI E RESPONSABILITÀ

L'utente è responsabile della propria postazione informatica e della casella di Posta Elettronica Personale.

L'utente è responsabile della segretezza del proprio user ID e relativa Password. È anche responsabile del contenuto dei messaggi inviati dalla propria casella elettronica.

L'utente si impegna a comunicare alla **UOC IngInf**, non appena ne venisse a conoscenza, qualsiasi uso non autorizzato da parte di terze persone del proprio user ID così come sono obbligati a segnalare immediatamente alla stessa UOC ogni sospetto di effrazione, incidente, abuso o violazione della sicurezza.

Gli utenti sono responsabili per la protezione dei dati utilizzati e/o memorizzati nei sistemi in cui hanno accesso; è fatto loro divieto di accedere direttamente o indirettamente a directory, files e servizi non espressamente e preventivamente autorizzati dalla Azienda.

Gli utenti sono tenuti a mantenersi aggiornati, controllando periodicamente le direttive della **UOC IngInf** divulgate tramite e-mail, sito intranet o circolare.

I responsabili delle Unità Operative e/o Servizi Aziendali dovranno adottare misure idonee per un corretto utilizzo delle risorse informatiche messe a disposizione della loro struttura, esercitando una funzione di istruzione, indirizzo e controllo sugli utenti incaricati ed individuando con precisione le responsabilità per la gestione dei dati, dei salvataggi e delle risorse stesse.

In caso di cessazione del rapporto di lavoro, trasferimento ad altro servizio, o comunque di non necessità di utilizzo da parte di utenti già autorizzati, il relativo Responsabile darà tempestiva comunicazione scritta, per gli applicativi da esso gestiti, alla **UOC IngInf** che provvederà alla disattivazione delle credenziali di autenticazione ovvero alla loro modifica per ogni diversa esigenza.

La **UOC IngInf** è responsabile della sicurezza, della funzionalità e del corretto impiego delle risorse informatiche centralizzate e della rete aziendale. Non rientrano nelle proprie competenze la gestione e l'assistenza tecnica delle apparecchiature elettromedicali e dei sistemi informatici di quelle unità operative (Laboratorio Analisi, Radiologia, Centro Trasfusionale, Anatomia Patologica, Sert etc.) che ospitano nelle loro sedi i server dedicati.

La gestione e responsabilità di questi ultimi è demandata ai singoli direttori che provvedono alla verifica ed alla corretta applicazione delle misure minime di sicurezza.

Per le postazioni personal computer "stand alone", ossia non collegate in rete, la responsabilità nell'applicazione delle misure minime di sicurezza è demandata all'utente finale ed al direttore dell'Unità Operativa/Sevizio che le ha in dotazione.

U.O.C. Ingegneria Informatica.
Direttore ing. Salvatore Garozzo

COMPORTAMENTI NON CONSENTITI NELLA "NAVIGAZIONE" IN INTERNET

Si rammenta, come già previsto nel regolamento Aziendale di cui alla Deliberazione n. 134 del 29 gennaio 2010, che non è consentito:

- l'utilizzo di modem personali e/o di access point;
- utilizzo di qualunque altro dispositivo "internet-Key" con account personali;
- navigare in internet in siti non attinenti allo svolgimento delle mansioni assegnate;
- l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di acquisti on line e simili, salvo casi espressamente autorizzati dalla Direzione Aziendale;
- il download di software gratuiti e shareware prelevati da siti internet, salvo casi espressamente autorizzati dalla Direzione Aziendale;
- ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa;
- la partecipazione, per motivi non professionali a Forum, l'utilizzo di Chat line, di bacheche elettroniche e le registrazioni in guest book anche utilizzando pseudonimi (nickname);
- la memorizzazione di documenti informatici di natura oltraggiosa e/o discriminatoria per sesso, lingua, religione, razza, origine etnica, condizioni di salute, opinione e appartenenza sindacale e/o politica;
- l'uso e la navigazione su siti di tipo Xrated, Casinò virtuali, Webchat basare su java, siti Warez e similari;
- l'uso di software di tunneling di qualsiasi natura o tipo.
- scaricare/scambiare materiale coperto da diritto d'autore;
- eseguire o favorire pratiche di Spamming

COMPORTAMENTI NON CONSENTITI NELL'UTILIZZO DELLA POSTA ELETTRONICA

Non è consentito:

- usare il servizio per scopi illegali, per inviare e ricevere materiale pedopornografico, osceno, volgare, diffamatorio, oltraggioso, discriminatorio, abusivo, pericoloso;
- utilizzare l'indirizzo di posta elettronica per la partecipazione a dibattiti, Forum o mailing-list per motivi non professionali;
- aderire o rispondere a messaggi che invitano ad inoltrare e perpetuare verso ulteriori indirizzi mail contenuti o documenti oggetto delle cosiddette "catene di S. Antonio"; (se si dovessero peraltro ricevere messaggi di tale tipo, si deve comunicarlo immediatamente al personale della **UOC IngInf**. Non si dovrà in alcun caso procedere all'apertura degli allegati a tali messaggi).
- effettuare ogni genere di comunicazione finanziaria ivi comprese le operazioni di remote Banking, acquisti on line e simili, salvo diversa ed esplicita autorizzazione aziendale;
- simulare l'identità di un altro utente, ovvero utilizzare credenziali di posta, non proprie, per l'invio di messaggi;
- prendere visione della posta altrui;
- aprire allegati di posta elettronica ambigui o di incerta provenienza (gli allegati possono, infatti, contenere virus o codici nascosti di natura dolosa che possono comportare la divulgazione di password o il danneggiamento di dati);
- modificare la configurazione hardware e software della sua macchina; né utilizzare sistemi client di posta elettronica non conformi a quelli accettati dall'azienda;
- l'utilizzo di critto sistemi o di qualsiasi altro programma di sicurezza e/o crittografia non previsto esplicitamente dal servizio informatico aziendale;
- l'invio di informazioni o documentazioni ad Istituti, Enti pubblici o privati, Associazioni, Comuni, Regioni senza previa autorizzazione della Direzione Aziendale
- la trasmissione a mezzo posta elettronica di dati sensibili, personali e/o commerciali di alcun genere se non nel rispetto delle norme sulla disciplina del trattamento e della protezione dei dati;

In caso di violazione o inadempimento di quanto riportato la Direzione aziendale procederà al distacco dell'utente dal collegamento ad internet e ne darà comunicazione per l'eventuale accertamento di responsabilità disciplinari del personale dipendente.

GESTIONE DEGLI INDIRIZZI

Gli indirizzi di posta elettronica per le strutture aziendali, condivisi da più operatori assegnati a ciascuna di esse sono attivati con la seguente nomenclatura:

nomestruttura@aspct.it.

Per le caselle personali gli indirizzi di posta elettronica, fatto salvi i casi di omonimia o esigenze particolari hanno la seguente nomenclatura:

nome.cognome@aspct.it

La "personalizzazione" dell'indirizzo non comporta la sua "privatezza", in quanto trattasi di strumenti di esclusiva proprietà aziendale, messi a disposizione del dipendente al solo fine dello svolgimento delle proprie mansioni lavorative.

Ciascun operatore può, anche da postazioni esterne all'azienda, utilizzare il sistema di posta elettronica.

CONTROLLI

I controlli saranno svolti in conformità alla legge, anche saltuari o occasionali, sia per eseguire verifiche sulla funzionalità e sicurezza del sistema sia per verificare il corretto utilizzo da parte dei propri dipendenti tanto della rete internet che della posta elettronica.

Nell'esercizio del potere di controllo l'Azienda si atterrà al principio generale di proporzionalità e non eccedenza delle attività di controllo, rispettando le procedure di informazione/consultazione delle rappresentanze dei lavoratori previste dai contratti collettivi e informerà preventivamente i lavoratori dell'esistenza di dispositivi di controllo atti a raccogliere i dati personali.

Le informazioni trattate infatti contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili ed in più le informazioni di carattere personale trattate possono riguardare, oltre all'attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell'uomo, "*può essere tracciata a volte solo con difficoltà". "Il luogo di lavoro è infatti una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l'esplicazione della per-*

sonalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali" (artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l'art. 2, comma 5, Codice dell'amministrazione digitale (D.Lgs. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l'uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato).

I controlli si svolgeranno in forma graduata:

1. In via preliminare l'Azienda provvederà ad eseguire dei controlli su dati aggregati, riferiti all'intera struttura lavorativa ovvero a sue aree e dunque ad un controllo anonimo che può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l'invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L'avviso può essere circoscritto a dipendenti afferenti all'area o settore in cui è stata rilevata l'anomalia.
2. In assenza di successive anomalie non si effettueranno controlli su base individuale;
3. Nel perdurare delle anomalie si procederà a controlli su base individuale o per postazioni di lavoro e in caso di abusi singoli e reiterati si eseguiranno controlli nominativi o su singoli dispositivi e/o postazioni di lavoro (indicando le ragioni legittime, specifiche e non generiche, per cui i controlli verrebbero effettuati - anche per verifiche sulla funzionalità e sicurezza del sistema - e le relative modalità - inoltrando preventivi avvisi collettivi o individuali);
4. In caso in cui la posta elettronica e la rete Internet siano utilizzate indebitamente o di riscontrato e reiterato uso non conforme delle risorse informatiche, la **UOC IngInf**, che effettua i controlli, segnalerà il comportamento al responsabile della struttura di appartenenza del dipendente.
5. Per il personale non dipendente cui non è applicabile il C.C.N.L. il comportamento andrà segnalato alla Direzione Aziendale per l'adozione degli atti di specifica competenza.

INTERRUZIONE E CESSAZIONE DELL'ACCESSO INTERNET

Eventuali interruzioni del servizio sono comunicate agli utenti.

U.O.C. Ingegneria Informatica.
Direttore ing. Salvatore Garozzo

Ai sensi del presente regolamento, l'utilizzo del servizio di accesso ad internet e di utilizzo di posta elettronica cessa d'ufficio nei seguenti casi:

- se non sussiste più la condizione di dipendente o collaboratore autorizzato o non è confermata l'autorizzazione all'uso;
- se è accertato un uso non corretto del servizio da parte dell'utente o comunque un uso estraneo ai suoi compiti professionali;
- se vengono sospettate manomissioni e/o interventi sul hardware e/o sul software dell'utente impiegati per la connessione compiuti eventualmente da personale non autorizzato;
- in caso di diffusione o comunicazione imputabili direttamente o indirettamente all'utente, di password, procedure di connessione, indirizzo I.P. ed altre informazioni tecniche riservate;
- in caso di accesso doloso dell'utente a directory, a siti e/o file e/o servizi da chiunque resi disponibili non rientranti fra quelli per lui autorizzati e in ogni caso qualora l'attività dell'utente comporti danno, anche solo potenziale al sito contattato;
- in caso di concessione di accesso ad internet diretta o indiretta a qualsiasi titolo da parte dell'utente a terzi;
- in caso di violazione e/o inadempimento imputabile all'utente di quanto stabilito nei precedenti punti.
- in ogni altro caso in cui sussistono ragionevoli evidenze di una violazione degli obblighi dell'utente.

DICHIARAZIONE DI ASSUNZIONE DI RESPONSABILITÀ PER L' ACCESSO A INTERNET DALLE POSTAZIONI AZIENDALI

(Dichiarazione da sottoscrivere e trasmettere alla **UOC IngInf**)

Qualora l'utente acceda a Internet tramite la rete dell'Azienda, è tenuto a sottoscrivere la dichiarazione di assunzione di responsabilità e acquisisce lo status di responsabile per la gestione e l'utilizzo della risorsa stessa;

INFORMATIVA ai sensi dell'art. 13 D.L.vo 196/03.

U.O.C. Ingegneria Informatica.
Direttore ing. Salvatore Garozzo

L'ASP Catania è **TITOLARE** del trattamento dei dati personali relativo all'utilizzo di strumenti elettronici da parte dei lavoratori.

FINALITA' del trattamento è la verifica del corretto utilizzo delle risorse informatiche, della posta elettronica e della rete Internet nel rapporto di lavoro.

MODALITA' del trattamento: gli operatori della **UOC IngInf** o personale tecnico autorizzato, effettueranno il trattamento dei dati secondo la normativa vigente, utilizzando strumenti informatici.

Il sottoscritto, firmando il presente documento, riconosce di aver letto, compreso ed accettato integralmente le politiche e le regole della ASP Catania, riguardo l'utilizzo della posta elettronica e l'accesso a Internet ; il sottoscritto si assume inoltre la piena responsabilità in caso di violazione delle leggi e dei regolamenti riconducibili al suo accesso personale.

Cognome e Nome : ……..

Luogo e Data di nascita : ……..

Matricola: ……. Telefono: …… fax:……

Settore/Distretto/Presidio Ospedaliero/UO :

……..

Indirizzo della sede :

..……..

Firma :

..……..

Autorizzazione del responsabile delle struttura: _____

Con la presente si richiedono le credenziali per l'acceso ad internet.

OSSERVANZA DELLE DISPOSIZIONI IN MATERIA DI PRIVACY

È obbligatorio attenersi alle disposizioni in materia di Privacy e misure minime di sicurezza D.Lgs. n. 196/2003, come indicato nel regolamento aziendale di cui alla Deliberazione n. 134 del 29 gennaio 2010.

DISPOSIZIONI FINALI

U.O.C. Ingegneria Informatica.
Direttore ing. Salvatore Garozzo

1. Il presente regolamento è stato sottoposto alla approvazione del Commissario Straordinario dell'Azienda che lo ha approvato con atto deliberativo.
2. La sua divulgazione avverrà nelle seguenti forme:
    a. trasmissione per posta elettronica a tutti i Dirigenti Responsabili di Presidio Ospedaliero, di Distretto Sanitario, di Dipartimenti e Uffici di Staff;
3. E' fatto obbligo a chiunque spetti di osservarlo.
4. Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni motivate al presente Regolamento. Le proposte verranno esaminate dalla Direzione Aziendale.

Ogni azione che non sia comunque conforme allo spirito del presente Regolamento, verrà considerata una violazione della sicurezza, e come tale comporterà la segnalazione alla Direzione Aziendale.